De 23 a 26 de outubro de 2018
ISBN 978-85-459-1280-4
Anais

BLOCKCHAIN: UMA DISCUSSÃO SOBRE VULNERABILIDADES E PERSPECTIVAS FUTURAS

Fernando Costa Leite[1]; Pietro Martins de Oliveira[2]

[1]Acadêmico do Curso de Análise e Desenvolvimento de Sistemas, UNICESUMAR, Educação à Distância (EAD). Bolsista do Programa de Iniciação Cientifica do Instituto Cesumar de Ciência, Tecnologia e Inovação PIC/ICETI.
[2]Orientador, Mestre, Professor Titular da UNICESUMAR, Maringá-PR.

RESUMO: O presente trabalho tem por objetivo estudar, analisar o funcionamento e reconhecer eventuais falhas dos algoritmos do *blockchain* da plataforma Ethereum. O *blockchain* é a base de funcionamento do Bitcoin e de outros criptoativos, dentre elas o próprio Ethereum. Sabe-se que bancos e governos de todo o mundo estão realizando experiências para adaptar seus sistemas com o intuito de utilizá-los em conjunto com a tecnologia *blockchain*, visto que sua utilização pode trazer inúmeros benefícios, tais como: rastreamento de transações registradas de maneira imutável e resistente a fraudes; inclusão de pessoas desbancarizadas; resguardar dados dos clientes da rede; entre outros. A tecnologia *blockchain* utiliza o conceito de *proof-of-work* (que consiste na geração do código de *hash* do bloco em produção) para validar transações. A prevenção de ataques cibernéticos como DDOS e Spam advém do caráter distribuído dos protocolos que utilizam *blockchain*. Além disso, algoritmos de criptografia, que se pretende estudar neste projeto, introduzem ainda mais segurança e também privacidade aos protocolos de consenso. Entretanto, eventuais vulnerabilidades do referido sistema podem levar a invasões e fraudes, justificando a realização deste trabalho. Em suma, o *blockchain* pode ser definido como um banco de dados descentralizado e distribuído que mantém um registro global de todas as transações ocorridas, em estruturas de dados denominadas blocos. Cada bloco é ligado ao bloco anterior formando uma cadeia de blocos, uma *blockchain*. Todo bloco contêm o seu próprio, e único, código *hash*. Um código *hash* pode ser definido como uma cadeia de caracteres gerados por uma função, denominada função de *hash*. Conceitos relacionados a Ciência da Computação, Redes de Computadores, Criptografia, Teoria dos jogos e Teoria Monetária dão indícios de possíveis vulnerabilidades que poderão ser encontradas através do presente trabalho. De acordo com o estado da arte, percebe-se claramente que o *blockchain* funciona como um protocolo de consenso que digitaliza a confiança em ambientes hostis. A confiabilidade dos criptoativos está diretamente relacionada com o poder de processamento de sua rede descentralizada, e pode ser perdida caso algum agente malicioso consiga atingir mais da metade do poder de processamento da rede, chamado de "ataque de 51%". A metodologia a ser empregada é baseada no método dedutivo, através de uma pesquisa exploratória na bibliografia correlata e nos próprios algoritmos evolvidos nessa tecnologia. Ao final do presente trabalho pretende-se verificar quais vulnerabilidades já foram identificadas e corrigidas dentro da *blockchain* Ethereum, e se essa plataforma ainda possui alguma falha de segurança a ser explorada. A escolha da *blockchain* da plataforma Ethereum se deve por ela prover suporte aos *Smarts Contracts*. Em linhas gerais, um *Smart Contract* é um protocolo computacional auto executável, com o intuito de permitir que novas aplicações possam ser desenvolvidas sobre uma *blockchain*. Os *Smart Contracts* podem ser uma potencial fonte de vulnerabilidades e serão estudados a fundo neste trabalho.

PALAVRAS-CHAVE: *Blockchain*, Ethereum, vulnerabilidades, consenso, segurança.